

**REQUEST FOR INTERFERENCE
WITH OTHER APPLICATIONS**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Richard Selinfrend et al.		
Serial No.:	TBA	Art Unit:	TBA
Filed:	Current Herewith	Examiner:	TBA
For:	Storage Media Access Control Method and System		

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR INTERFERENCE UNDER 37 C.F.R. § 1.604

Sir:

Applicant requests that an interference be declared between the above-captioned application and applications serial nos.: 10/023,424 filed on December 12, 2001 and published August 22, 2002 (US2002/0114265 A1); 09/960,610 filed on September 21, 2001 and published August 29, 2002 (US2002/0120854 A1); 09/989,910 filed on November 20, 2001 and published on October 3, 2002 (US2002/0144153 A1); and 10/062,400 filed on February 1, 2002 and published on March 6, 2003 (US2003/0046545 A1). The proposed counts of the interference are:

COUNT 1

A method for modifying an optical path of an optical medium, the optical medium including a first layer adjacent a data layer comprising: selecting a region of the first layer to be distorted; and distorting the region of the first layer such that a reading operation of data stored in the first layer corresponding to the distorted region is modified;

optionally wherein: (1) the steps of selecting a region and distorting the region are performed on the reading layer; (2) selecting comprises selecting a predetermined region of the first layer; (3) selecting comprises selecting a random region of the first layer;

and further optionally wherein: (1) the first layer comprises the reading layer through which the optical path is directed; (2) the optical medium further comprises a back layer adjacent the data layer, opposite the reading layer; (3) the distortion alters the optical path of the incident light for reading the corresponding data in the data layer.

COUNT 2

A method for preventing unauthorized use of digital content data stored on a medium comprising: determining one or more data segments in the digital content data, modifying one or more of such data segments to generate modified data comprising second data; storing the modified data at predetermined memory locations on the medium;

optionally wherein: (1) the digital data comprises data types selected from a group consisting of: audio, video, documents, text or software; (2) the data segments are of variable length; (3) the second data comprises portions of the digital content data; (4) the modified data comprises encrypted data.

COUNT 3

A method for preventing unauthorized use of digital content data to be transferred from a first system to a second system comprising: locating an archive of a digital content data at the first system; determining transaction data of the second system; determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the archive; and transferring the archive from the first system to the second system if the second system is a valid recipient;

optional comprising the step of, if the second system is not a valid recipient after transfer of the archive from the first system to the second system, the operation of the archive failing in the second system; and

optionally: (1) wherein the first system comprises optical medium or other hard medium, while the second system comprises a computer on the network or a computer system; (2) wherein both the first and

second system comprise computers/computer system; (3) wherein the first and second computers/computer systems are remotely located.

COUNT 4

A method for authenticating a digital medium comprising: monitoring a transfer rate of read data resulting from the reading of valid data stored on a digital medium at a physical location; determining, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical location of the valid data on the digital medium; and authenticating the digital medium based on a characteristic of the anomaly region.

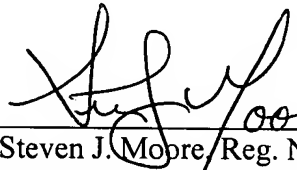
COUNT 5

A system for authenticating a digital medium comprising: a monitor for monitoring a transfer rate of read data resulting from the reading of valid data stored on a digital medium at a physical location; an anomaly detector for determining, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical location of the valid data on the digital medium; and an authenticator for authenticating the digital medium based on a characteristic of the anomaly region.

Claims 1 - 7 of the above identified application and claims 1- 3, and 7 - 10 of U.S. Patent Application No. 10/023,424 substantially correspond to Count 1. Claims 8 and 10 - 13 of the above identified application correspond to claims 1 – 3, and 5 – 6 of U.S. Patent Application No. 09/960,610 substantially correspond to Count 2. Claims 14 – 18 of the present application and claims 1 – 5 of U.S. Patent Application No. 09/989,910 substantially correspond to Count 3. Claim 19 of the identified application and claim 1 of U.S. Patent Application No. 10/062,400 substantially correspond to Count 4. Claim 20 of the identified application and claim 56 of U.S. Patent Application No. 10/062,400 substantially correspond to Count 5.

An interference is believed to be necessary because the same invention is being claimed in these applications and priority cannot be determined without an interference.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Steven J. Mopre', written over a horizontal line.

8/21/03

Steven J. Mopre, Reg. No. 35,959
PILLSBURY WINTHROP LLP
695 East Main Street, Suite A3
Stamford, CT 06901
Tel.: (203) 965-8254
Fax: (203) 965-8226